

ORIGINAL FILED

1 JAMES R. BUSSELLE (SBN 75980)
2 THOMAS E. MOORE III (SBN 115107)
3 MARY E. O'BYRNE (SBN 121067)
4 TOMLINSON, ZISKO, MOROSOLI & MASER
5 200 Page Mill Road, Second Floor
6 Palo Alto, California 94306
7 Telephone: (415) 325-8666

Nov 15 3:31 PM '95

RICHARD W. WIEKING
CLERK
U.S. DISTRICT COURT
NO. DIST. OF CA. S.J.

8 Attorneys for Defendant
9 RSA Data Security, Inc.
10

11 UNITED STATES DISTRICT COURT
12 NORTHERN DISTRICT OF CALIFORNIA
13

14 ROGER SCHLAFLY,

) CASE NO.: C 94 20512 SW (PVT)

15 Plaintiff,

) DECLARATION OF RONALD L.
16 vs.) RIVEST IN OPPOSITION TO
17) PLAINTIFF'S MOTION FOR
18) PARTIAL SUMMARY JUDGMENT

PUBLIC KEY PARTNERS and RSA DATA)
SECURITY, INC.,

) DATE: December 6, 1995

Defendants.

) TIME: 10:00 a.m.
19 BEFORE: Hon. Spencer
20 Williams
21

22 I, Ronald L. Rivest, declare:

23 1. I am one of the inventors of U.S. Patent No.

24 4,405,829, "Cryptographic Communications System and Method" (the
25 "MIT Patent"), and I am one of the founders of defendant RSA Data
26 Security, Inc. I have personal knowledge of each and every fact
27 set forth below and can competently testify thereto.

28 2. I received a B.A. degree in Mathematics from Yale
University in 1969, and a Ph.D. degree in Computer Science from
Stanford University in 1974. I am presently a professor of
computer science at the Massachusetts Institute of Technology
("MIT"), and I am also the associate director of MIT's Laboratory

TOMLINSON, ZISKO, MOROSOLI & MASER
ATTORNEYS AT LAW
200 PAGE MILL ROAD, SECOND FLOOR
PALO ALTO, CALIFORNIA 94306
(415) 325-8666

for Computer Science, a member of MIT's Theoretical Computer Science Group and a co-founder of MIT's Cryptography and Information Security Group. I am a member of the ACM and the National Academy of Engineering and I have served as a director of the International Association of Cryptologic Research, the organizing body for the EUROCRYPT and CRYPTO series of technical conferences on cryptology for many years. I have also published numerous papers in the areas of cryptographic design and cryptanalysis.

3. Cryptography is the study of codes and ciphers to ensure the privacy and authentication of information. Over its history, cryptographic techniques and design have evolved to meet technological improvements both in communications and in methods of cryptanalysis, i.e. code breaking.

4. The use of secret codes for military applications goes back thousands of years. Julius Caesar is known to have used a secret code involving the simple replacement of each letter of a message by the letter three places down in the alphabet: For the letter "A," Caesar used the letter "D," for the letter "B," Caesar used the letter "E," etc. The specific parameters of the Caesar code, that is, the shift of three letters down the alphabet, is referred to as the "key." The original message is referred to as "plaintext" and the encoded message is referred to as "ciphertext." Because the security of Caesar's key depended on its not being known to Rome's enemies, such a key is referred to as a "secret key."

5. The Caesar key has two inherent weaknesses. First, it is a very simple letter-substitution key. Systematic methods of

1 breaking such a key are almost as old as cryptography itself.
2 Second, Caesar's secret key was exposed to possible interception
3 every time the secret key was changed or new users of the secret
4 key were added.

5 6. The first weakness of the Caesar key illustrates the
6 essential challenge of cryptographic design. To ensure security,
7 code-makers have to stay at least one step ahead of the code-
8 breakers. As a consequence, over the centuries, code design has
9 of necessity become increasingly complex. This challenge was
10 increased with the advent of expanded communications technology.
11 Radio signals permitted military forces to communicate with each
12 other over long distances. Radio also allowed anyone tuned in to
13 the right frequency to intercept numerous coded messages. The
14 more coded messages available for cryptanalysis, the easier the
15 task of breaking the code becomes.

16 7. The same problem exists for any communications signal
transmitted over an insecure channel. Further examples are tele-
17 phone wires which can be tapped, cellular telephone conversations
18 which can be overheard, satellite signals which can be inter-
19 cepted and computer-to-computer communications over the Internet
20 which a clever hacker can retrieve.

22 8. To accomplish greater complexity and to accommodate
23 technological improvements in communications, cryptographic
24 design turned to the use of encryption machines. Perhaps the
25 best known encryption machine was the German "Enigma" machine of
26 World War II. The Enigma used varying combinations of rotors to
27 encrypt and decrypt messages. With considerable effort and some
28 luck, the Allies finally broke the Enigma during the war.

1 9. If the Enigma were in use today, however, modern
2 computers, applying appropriate techniques, would have made short
3 work of breaking it. Modern cryptographic design must not only
4 accommodate technological advances in communications, it must
5 also accommodate the ever-increasing processing speed of compu-
6 ters. Because of this, modern cryptographic design, and the
7 machines used to implement those designs, are inextricably
8 linked. These machines include: microchips designed to encrypt
9 data sent over telephone lines, and general purpose computers
10 using specially-designed software.

11 10. Patents have been granted on encryption machines for
12 decades. Most of these patents describe a means of inputting
13 plaintext (the original message) and outputting ciphertext (the
14 encoded message), often over some form of communications channel.
15 The patents describe, often in mathematical terms, the internal
16 workings of encryption machines as a key or means of creating
17 keys (known as "key generation"). A true and correct copy of
18 several pages of a list of cryptography patents is attached
19 hereto as Exhibit A.

20 11. The other weakness inherent in Caesar's secret key is
21 common to all secret key systems, namely the risk of interception
22 when secret keys are distributed. The nature of the risk of
23 interception has changed as the market for cryptography has
24 grown. The advent of computers and advanced telecommunications
25 has expanded the market for cryptography beyond military and
26 other governmental uses. Private industry has developed a need
27 to protect personal and corporate privacy because competitors can
28 easily intercept telephone conversations (particularly over

1 cellular phones), electronic messages, faxes and satellite
2 transmissions.

3 12. "Public key" cryptography was invented to solve these
4 problems. In public key cryptography, every user has two keys
5 (rather than one), a public key and a private key. The public
6 key can be published for all the world to see and use. The
7 private key is kept in strict confidence by its owner. For the
8 system to work successfully, this pair of keys must have two
9 properties:

10 (a) Anything encrypted with one key can be decrypted with
11 the other; and

12 (b) Given the knowledge of the public key, it is infeasible
13 to discover the private key.

14 Thus, for Alice to send a coded message to Bob, Alice looks up
15 Bob's public key in a directory of public keys. Alice encrypts
16 the message with Bob's public key. When Bob receives the
17 message, he decrypts the message with his own private key.
18 Because it is infeasible for Alice or anyone else to take Bob's
19 public key and use it to discover Bob's private key, privacy of
20 the message is assured.

21 13. Public key cryptography also allows the use of
22 "digital signatures" that verify the identity of a sender in much
23 the same way that a real signature validates a check or contract.
24 Alice can "sign" her message to Bob by using her own private key
25 to create the "signature." Again, this private key is unique to
26 Alice. Bob may then use Alice's public key to confirm that the
27 "signature" was created with Alice's private key. This confirms
28 that Alice sent the message.

1 14. The unique qualities of public key cryptography are
 2 expanding the cryptography market still further. Various
 3 companies are touting electronic cash, checks and credit cards,
 4 by which ordinary consumer transactions take place via computer
 5 over the Internet. To accomplish this, the transactions must be
 6 both secure and authenticated. Public key cryptography provides
 7 a means for an ordinary consumer to encrypt information such as a
 8 credit card number before releasing it over telephone lines and,
 9 through digital signatures, provides a means for the recipient of
 10 the information to confirm the identity of the sender.

11 15. In and around 1977, Adi Shamir, Leonard M. Adleman and
 12 I worked together at MIT. We spent months creating the invention
 13 described in the MIT Patent, as a particular implementation of
 14 public key cryptography.

15 16. We filed our application for a patent with the Patent
 16 and Trademark Office on December 14, 1977. The patent was not
 17 issued until almost six years later, on September 20, 1983.
 18 During that period, our application was carefully scrutinized,
 19 particularly on the subject of patentability. At one point in
 20 1979, the patent examiner even rejected the application on the
 21 grounds that it contained a mathematical algorithm. This
 22 rejection was later reconsidered and withdrawn. A true and
 23 correct copy of the brief filed by our patent counsel seeking
 24 such reconsideration is attached hereto as Exhibit B. A true and
 25 correct copy of the final, issued patent is attached to the
 26 Declaration of Thomas E. Moore III as Exhibit C.

27 17. Dr. Shamir, Dr. Adleman and I assigned the patent to
 28 MIT. At about that time, the three of us formed defendant RSA

TOMLINSON, ZISKO, MOROSOLI & MASER
ATTORNEYS AT LAW
200 PAGE MILL ROAD, SECOND FLOOR
(415) 325-8666
PALO ALTO, CALIFORNIA 94306

1 Data Security, Inc. ("RSA"). The letters "RSA" come from the
 2 first initials of our last names. On or about September 29,
 3 1983, MIT granted to RSA an exclusive license to the Patent,
 4 together with the right to sue infringers of the MIT patent. RSA
 5 has marketed and licensed cryptographic software ever since. I
 6 understand that RSA's success stems in part from the perception
 7 that the technology that Dr. Shamir, Dr. Adleman and I invented
 8 is the most secure public key encryption and authentication
 9 method commercially available. In fact, in its more secure
 10 forms, a high-speed computer could take thousands of years to
 11 decipher a single message encrypted with the technology.

12 18. The MIT Patent describes an apparatus, system and
 13 method of public key cryptography. In basic terms, the system is
 14 a way of transforming plaintext message signals into ciphertext
 15 signals using certain steps, which are described with mathe-
 16 matical symbols. The plaintext and ciphertext message signals
 17 may be in the form of a telephone signal, a modem signal, a
 18 facsimile signal, a radio signal or other form capable of being
 19 carried over a communications channel.

20 19. The system makes use of the principle that finding
 21 prime numbers is computationally easy, but that factoring the
 22 product of two such numbers can be computationally infeasible,
 23 even for sophisticated computers. The system includes a
 24 communications channel coupled to at least one terminal having an
 25 encoding device and to at least one terminal having a decoding
 26 device. The public key is created by selecting two prime
 27 numbers, P and Q, and multiplying them together to obtain a
 28 composite modulus N.

TOMLINSON, ZISKO, MOROSOLI & MASER

ATTORNEYS AT LAW
200 PAGE MILL ROAD, SECOND FLOOR
PALO ALTO, CALIFORNIA 94306
(415) 325-8666

1 20. The composite modulus N, together with a suitably
 2 chosen enciphering exponent e, is provided to the message-sender
 3 (the owner of the encoding device), or to the public. The prime
 4 number factors, P and Q remain secret. The message-sender's
 5 encoding device encrypts the plaintext message signal using an
 6 electronic representation of the public information, e and N,
 7 creating a ciphertext message signal. This ciphertext message
 8 signal can only be decoded by persons in possession of the
 9 (electronic representations of) P and Q. Usually, this will be
 10 the intended recipient's decoding device, because it is that
 11 device which stored the (electronic representations of) the
 12 secret numbers P and Q.

13 21. The MIT Patent is not a "disembodied mathematical
 14 concept," "abstract idea" or a "law of nature." The MIT Patent
 15 is limited to communications systems that use a particular
 16 transformation that turns plaintext communication signals into
 17 ciphertext signals. Outside of encryption technology, the
 18 principles on which the MIT Patented technology depends remain
 19 available for all creative minds to use.

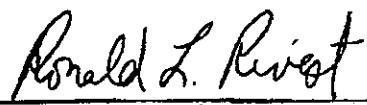
20 22. There are many descriptions of the MIT Patented tech-
 21 nology in published materials, some of which I have written.
 22 Often, these descriptions refer to the technology in mathematical
 23 terms. The reason for this is that mathematic expressions pro-
 24 vide a convenient, shorthand means of expressing the transfor-
 25 mation that occurs to the plaintext message signal when an encoding
 26 device turns that signal into an encrypted ciphertext signal.
 27 Without the mathematical shorthand, the descriptions of the

FROM : TEL: .15.1995 1:05 AM P 2
11/14/95 20:58 **D**415 324 1808 TZM&M **D**002

1 encryption transformation would necessarily involve cumbersome
2 descriptions of circuitry or software.

3 I declare under penalty of perjury under the laws of the
4 United States of America that the foregoing is true and correct.

5 Executed on November 15, 1995 at Cambridge, Massachusetts.

6 
7

8 Ronald L. Rivest

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTORNEYS AT LAW
200 PAGE MILL ROAD, SECOND FLOOR
PALO ALTO, CALIFORNIA 94303
(415) 325-8868

A

11/15/95

11:53

8617 258

12

LCS/AI MIT EDU

ZM&M

002

UNITED STATES
CRYPTOGRAPHIC PATENTS
1861 - 1981

JACK LEVINE

Cryptologia

Terre Haute

11/15/95 11:54 617 258 '82

LCS/AI MIT EDU → FZM&M

003

UNITED STATES CRYPTOGRAPHIC PATENTS: 1861-1981

by Jack Levine

This book is published by

CRYPTOLOGIA, Inc.
Rose-Hulman Institute of Technology
Terre Haute, Indiana 47803 USA.

First printing, February 1983.

Copyright 1983, by CRYPTOLOGIA, Inc.

ISBN 0-9610560-0-2.

Cover: Illustrations from Electric Coding Machine patent issued to E. H. Hebern.

Patent number 1,510,441 granted September 30, 1924.

11/15/95

11:54

617 258

'82

LCS/AI MIT EDU

ZM&M

004

UNITED STATES CRYPTOGRAPHIC PATENTS

TABLE OF CONTENTS

Preface	v
Introduction	vii
List of primary patents 1861-1981	1
List of secondary patents (by number only)	61
List of inventors with at least five patents	63

11/15/95 11:54 617 258 82

LCS/AI MIT EDU → ZM&M

005

UNITED STATES CRYPTOGRAPHIC PATENTS

Jan. 21, 1930.

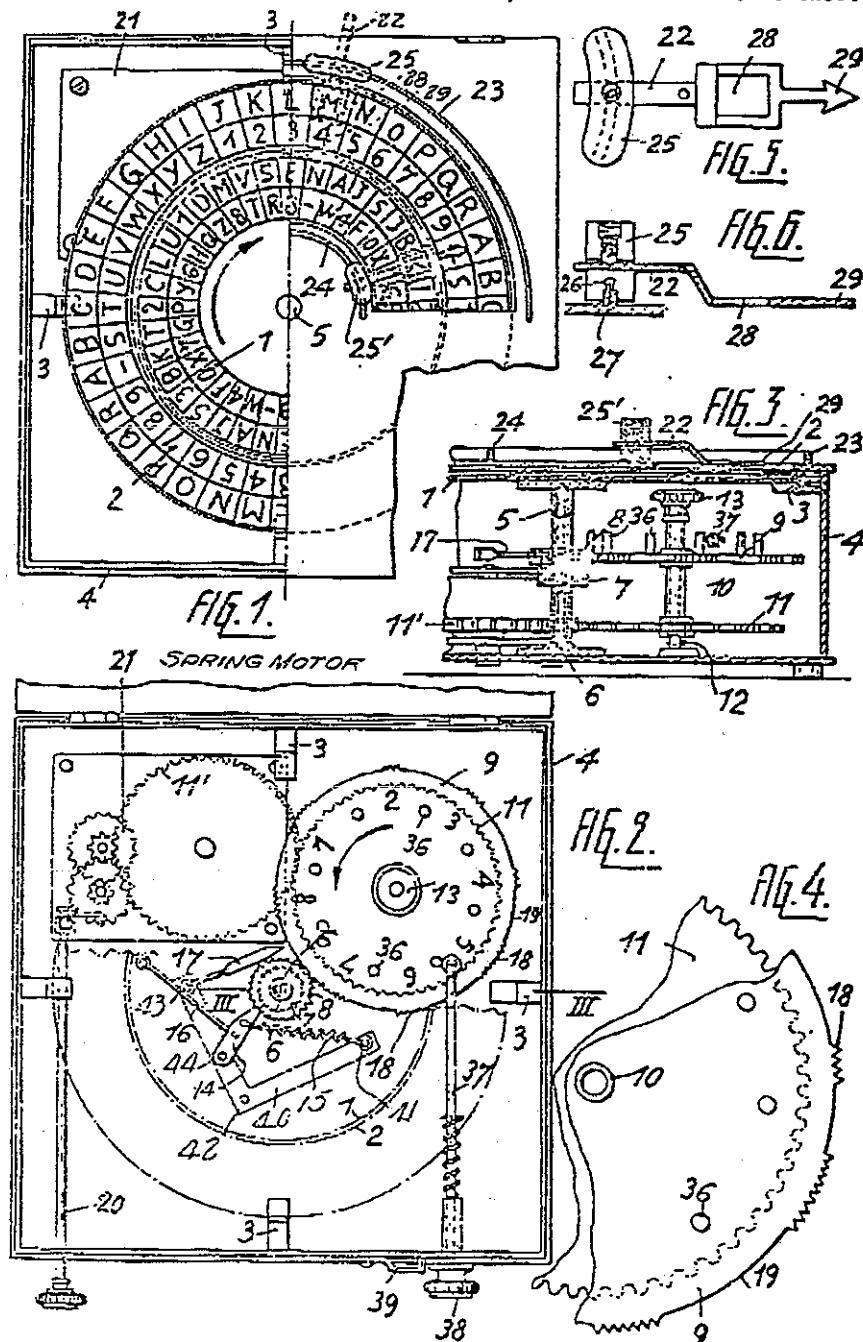
A. VON KRYHA

1,744,347

CODING MACHINE

Filed Feb. 20, 1925

2 Sheets-Sheet 1



Inventor
 A. von Kryha
 Marker Clark
 1930

11/15/95 11:55 617 258 32

LCS/AI MIT EDU ZM&M

4006

UNITED STATES CRYPTOGRAPHIC PATENTS

PREFACE

As my column on cipher equipment in Cryptologia attests, my favorite cryptologic topic is closely related to patents. Therefore, I am especially pleased to be able to add a few words to this exceptional work.

Years ago, before I was indoctrinated into the more sophisticated techniques of patent searching, I used to order patents by the dozen by picking patent numbers at random from lists of class numbers that I knew included cipher machines. When the patents arrived I was fascinated by the interesting and intricate drawings and also frustrated when I tried to decipher the descriptive material, which was written by lawyers who really did not want you to know how the device worked. I also had my disappointments when a patent turned out to be a check protection system, card validation method or in some other peripheral area.

Now, with the publication of this unique tome the veil is lifted and no longer will even the most inexperienced neophyte have to guess about the kind of patent being ordered. But more than that, this extraordinary compilation is a source-book for the study of cryptographic history, the development of cryptographic techniques and their inventors. It is the most complete listing of patents devoted to cryptology ever published and is the result of over 40 years of research by a mathematics professor who has already earned a reputation for excellence in cryptology with numerous papers in leading mathematics journals. Dr. Jack Levine's assiduous work in preparing the final manuscript can best be appreciated by one who was on the receiving end of a virtual torrent of letters which continually updated, improved and corrected what I thought was a fine job at the outset.

Only a labor of love could have produced a work of this quality and there is no doubt that it will remain the standard reference for cryptologic patents well beyond our lifetime and a lasting, well deserved tribute to Professor Jack Levine.

Louis Krüh
1 June 1982

11/15/95

11:55

617 258 82

LCS/AI MIT EDU → ZM&M

007

UNITED STATES CRYPTOGRAPHIC PATENTS

2 Sheets—Sheet 2.

(Model)

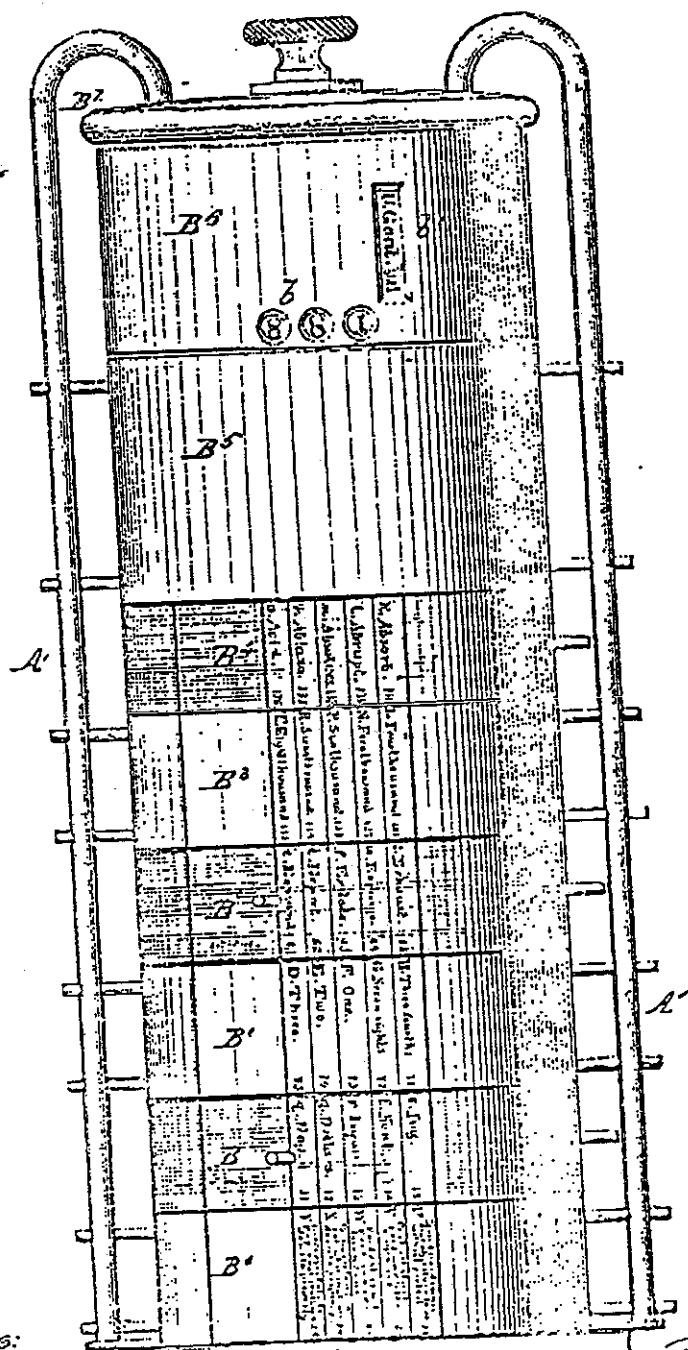
R. T. ONEY.

CIPHER CODE AND APPARATUS.

No. 266,876.

Patented Oct. 31, 1882.

Fig. 5.



Witnesses:

Phil C. Dietrich

Clyde Scott

Inventor:

R. T. Oney

Alexander
Dolmetsch

UNITED STATES CRYPTOGRAPHIC PATENTS

INTRODUCTION

The expression "cryptographic patent" in this paper means: (1) a device to convert intelligible information into an unintelligible form, or (2) components which are part of such devices.

Examples of information mentioned in (1) include written and spoken language, music, pictures, stock quotations, signaling. Also included in (1) are devices to prevent unauthorized television reception, and means for fraud prevention. These latter two are contained in the listings under "Cryptography" or "Secret" in the Patent Office publication Index to Patent Classification (see below).

Examples of (2) are rotors, key tapes, pseudo-random number generators. Patents relating to the television classification usually contain the expression "subscription television" in the title. A good example is the title of patent number 3,478,166. A large number of such patents have appeared beginning about 1950. Most of the inventions of two of the leading inventors (by frequency) have been in this television classification (see below for a list of the high-frequency inventors).

In the early years (centering around 1900) fraud prevention patents mainly dealt with protection of checks. About 1965 the idea of fraud prevention was greatly extended with patents in such areas as prevention of unauthorized use of credit cards (including automatic currency dispensing), and unauthorized computer access. These patents contain some form of encryption. What may be considered as the development of the traditional "cipher machine" covered the approximate period 1920-1950. Some of the better known names associated with this development include Friedman, Hagelin, Hebern, Kryha, Scherbius, Vernam. Somewhat previous to this time a popular form of patent involved the construction of small-size codes. An example of this may be found in patent number 832,156, and also in 832,559.

In the patent listing which follows the expression "primary patent" indicates a patent included in items (1) or (2) above. A much smaller list called "secondary," while not a member of (1) or (2), may perhaps by some variation in operation be converted to a primary patent. Most pulse code modulation patents are considered secondary, though there are some in the primary class. The secondary patents are listed by number only. The primary patents are displayed in the form

<u>Patent number</u>	<u>Name of inventor</u>	<u>Date granted</u>	<u>Title of patent</u>
----------------------	-------------------------	---------------------	------------------------

Some general information relative to publications of the Patent Office may be helpful to cryptographic patent searchers. A patent is classified by its class and subclass (CSC), and each patent is numbered. At the present time the numbers are in the four million range.

The Official Gazette of the U. S. Patent and Trademark Office (published weekly) contains a brief abstract of each patent granted for the particular week, and includes patent number, CSC, and usually a related diagram.

An Annual Index of Patents is published in two parts with an alphabetical list of patentees in Part I, and a list of patents arranged by CSC in Part II.

UNITED STATES CRYPTOGRAPHIC PATENTS

Two other important publications are:

Index to the U. S. Patent Classification, which lists alphabetically by subject matter (and subdivisions) the various class-subclass divisions of patents. Thus, under the subject "secret" is found (as one subdivision) "Telegraph" with CSC 178-22 (which has now been subdivided into nineteen subdivisions). The Manual of Classification which lists all CSC's in numerical order, together with the corresponding subject.

Other publications are Classification Definitions, containing in some detail information on the content of the class-subclasses; the Numeric Listing, a microfilm listing of patents in numerical order with corresponding CSC's; and a microfilm listing arranged by CSC, i.e., all patents with the same CSC are listed together.

In the Index to Patent Classification (dated December 1980), under headings "Cryptography" and "Secret" are listed:

CryptographyClass-subclass(es)

Code transmitters	178-79
Code receivers	178-89
Codes	178-113
Fraud preventing	283-11
Printed matter	283-17
Typewriting	400-89 and -90
Education	434-119 (through 125)

SecretClass-subclass(es)

Telegraph	178-22
Telephone	179-1.5R
Fiber optics	355-1
Photo copying	355-40
Television	358-114 (through 124)
Faximile	358-259
Radio, pulse or digital	375-2
Radio	455-26 (through 30)

The Manual also lists the following: 178-37 recorders, secret; 179-1.5C, recorder, 179-1.5E encoding, 179-1.5M masking, 179-1.5S scrambling, 179-1.5FS frequency shifting.

Remarks. The class-subclass of a patent is subject to change. For example, the cryptographic CSC of long-standing 197-4 (typewriter) is now 400-89 (mechanical) and 400-90 (electrical). The very old cryptographic CSC's 35-2, 35-3, 35-4 are now 434-119 (through 125). The CSC 325-32 (radio) is now 455-26 (through 30). The CSC 178-22 (telegraph) has now been subdivided into nineteen subclasses 178-22.01 through 178-22.19. More recent types of encipherments, such as "public-key" are included in these subdivisions.

UNITED STATES CRYPTOGRAPHIC PATENTS

Cryptographic patents may also have CSC's not listed above. Those which have been noticed are:

3,361,511	350-96.25
3,502,793	178-4
3,508,205	340-172.5
3,519,322	350-3.68
3,611,294	349-142
3,614,780	343-7ED

Any patent may be ordered from

Commissioner of Patents and Trademarks
Washington, D. C. 20231

at one dollar each, and should be ordered by the patent number.

The sections to follow contain the following:

- I. List of primary patents 1861-1981
- II. List of secondary patents (by number only)
- III. List of inventors with at least five patents

Also figures selected from various patents are distributed throughout.

Acknowledgments. The writer is very pleased to have this opportunity to express his thanks to Jean Porter, Head, Documents Department and to Stuart Basetsky, Assistant Head, Documents Department of the D. H. Hill Library, North Carolina State University, for their very generous help during the preparation of this work; to Dr. David Kahn whose advice many years ago was the incentive to continue with the enlargement of my then small patent collection; and to Louis Kruh whose valuable suggestions and constant encouragement made it possible to complete this difficult project.

UNITED STATES CRYPTOGRAPHIC PATENTS

W. J. ROUSSEL.

CIPHER CODE SYSTEM.

APPLICATION FILED SEPT. 1, 1908.

916,606.

Patented Mar. 30, 1909.

Fig. 2.

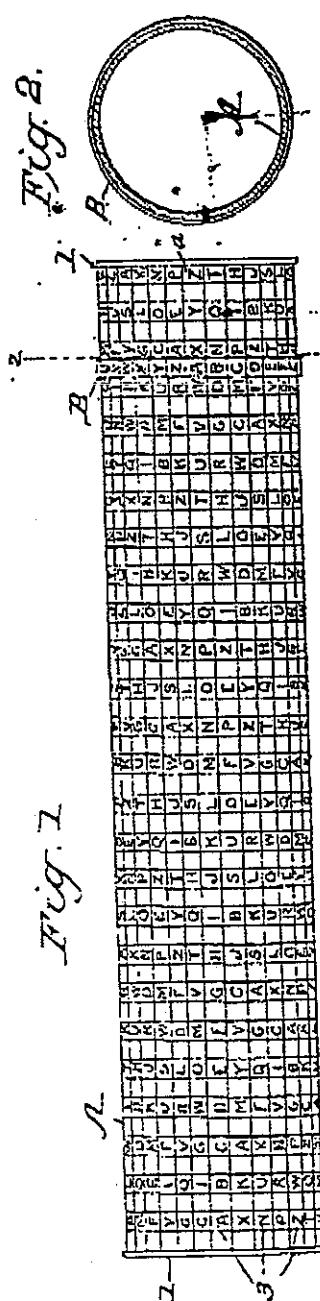
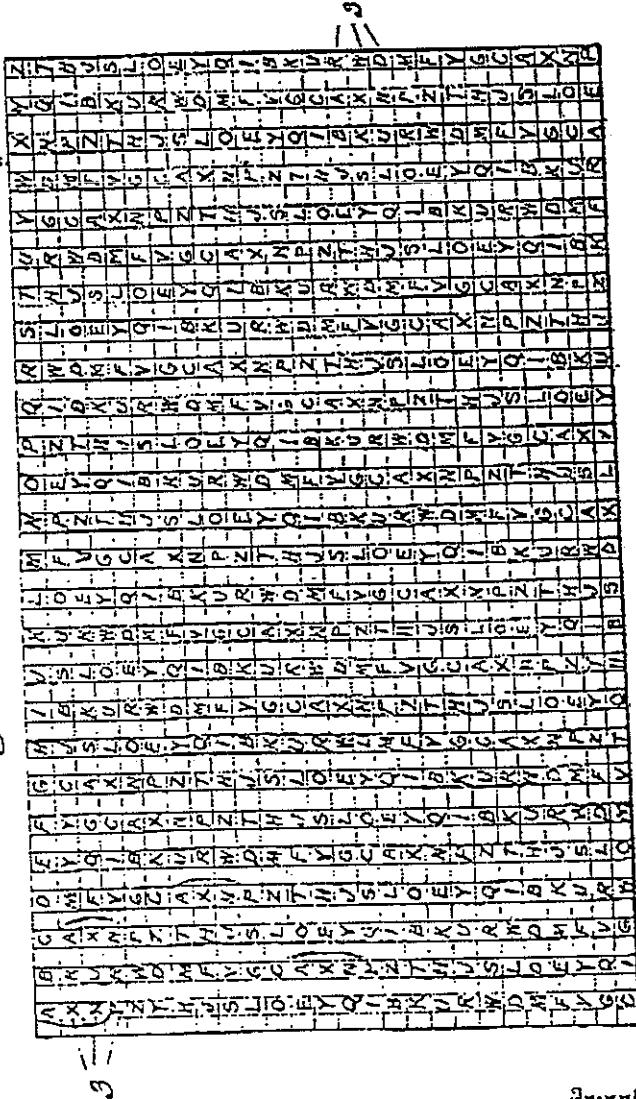


Fig. 3.

Fig. 3.



Inventor

Willie J. Roussel

Witnesses
Jos. A. Ryan
Victor J. Evans

Attorney

Jos. A. Ryan

Victor J. Evans

Attorney

UNITED STATES CRYPTOGRAPHIC PATENTS

LIST OF PRIMARY PATENTS 1861 - 1981

31,902 Alfred E. Parks	Apr 2 1861	Telegraphic register
32,854 Alexander Bain	Jul 23 1861	Electric acoustic telegraph
34,079 Asahel Ward	Jan 7 1862	Improvement in telegraphing by colors
37,997 Alexander Bain	Mar 24 1863	Dial telegraph
38,529 Alexander Bain	May 12 1863	Improvement in calls for telegraphs
39,016 Pierre Stanislas	Jun 23 1863	Improvement in telegraphic signals
40,744 George H. Felt	Dec 1 1863	Improvement in signal-codes for rockets
42,794 Henry J. Rogers	May 17 1864	Improvement in semaphoric telegraphs
43,763 Philip Colomb	Aug 9 1864	Improvement in apparatus for signaling
48,681 Edward H. Hawley	Jul 11 1865	Cryptographic alphabet
50,946 Albert J. Myer	Nov 14 1865	Improvement in signals
51,809 M. L. Deering	Jan 2 1866	Annunciator
58,562 F. J. Bolton	Oct 2 1866	Improvement in signal-codes for electric telegraphs
59,148 Ralph A. Jones et al.	Oct 23 1866	Improvement in telegraphic signals
68,088 Thomas W. Knox	Aug 27 1867	Improvement in transmitting plans of battle-fields by telegraph
112,836 Henry C. Nicholson	Mar 21 1871	Improvement in telegraph apparatus
156,851 Isaac Joseph et al.	Nov 17 1874	Improvement in cryptography
166,761 Anthony L. Flamm	Aug 17 1875	Improvement in cryptography
173,718 Thomas A. Edison	Feb 22 1876	Improvement in automatic telegraphy
180,096 Royal E. House	Jul 25 1876	Improvement in telegraphic codes or alphabets
185,621 Alexander Berghold	Dec 26 1876	Improvement in devices for secret writing
193,299 William A. Smith	Jul 17 1877	Method of preventing the alteration or counterfeiting of monetary papers
194,347 Fred. Grafelmann et al.	Aug 21 1877	Improvement in apparatus for testing bank checks, etc.
197,199 Frank S. Baldwin	Nov 20 1877	Improvement in cryptographic devices
217,478 David D. Gregory	Jul 15 1879	Improvement in bank-checks
238,566 Charles G. Burke	Mar 8 1881	Cryptography
251,292 James H. Rogers	Dec 20 1881	Telephony
253,060 Albert F. Johnson et al.	Jan 31 1882	Secret message telegraph
253,061 A. F. Johnson et al.	Jan 31 1882	Apparatus for preparing and transmitting secret telegraph messages
253,062 A. F. Johnson et al.	Jan 31 1882	Secret printing telegraph
253,063 A. F. Johnson et al.	Jan 31 1882	Secret printing telegraph
266,875 Robert T. Oney	Oct 31 1882	Cipher code and apparatus
268,237 A. F. Johnson et al.	Nov 28 1882	Printing telegraph
275,339 Albert F. Johnson et al.	Apr 3 1883	Automatic printing telegraph
281,006 Howard Bodey	Jul 10 1883	Check, draft, note and etc.
283,883 Timothy Gruaz	Aug 28 1883	Combination cipher
294,175 John L. Winnea	Feb 26 1884	Cryptographical table
295,855 Charles G. Burke	Mar 25 1884	Telegraphic system
312,665 David R. Smith	Feb 24 1885	Combination cipher-machine

UNITED STATES CRYPTOGRAPHIC PATENTS

335,929 Abram G. Hoyt	Feb 9 1886	Telegraphic code
343,044 Edward J. Mallett	Jun 1 1886	Automatic telegraphy
364,356 William A. Leggo	Jun 7 1887	Telegraphic alphabet
376,569 Samuel B. Whitehead	Jan 17 1888	Telegraphic apparatus
394,961 Mark W. Dewey	Dec 25 1888	Telegraphic printing code
396,529 Gustav Bofinger	Jan 22 1889	Typewriter ciphograph
407,425 Alexis von Simon	Jul 23 1889	Cryptographic apparatus
431,792 Frank Anderson	Jul 8 1890	Apparatus for preparing and translating secret messages
442,674 Marshall A. Wier	Dec 16 1890	Typewriter ciphograph
449,723 Marshall A. Wier	Apr 7 1891	Device for forming and deciphering secret communications
469,961 William B. Chalmers	Mar 1 1892	Signaling apparatus
470,871 C. Rymtowtt-Prince	Mar 15 1892	Type writing machine
478,294 Thomas S. Spivey	Jul 5 1892	Method of protecting bank checks and the like from being raised
492,677 Richard Harte	Feb 28 1893	Cryptographic instrument
495,744 Joseph Levi	Apr 18 1893	Method of indicating telegraphic messages
506,731 William R. Rothwell	Oct 17 1893	Cipher device
510,430 Wallace R. Kirk	Dec 12 1893	Telegraph or telephone system
527,112 Richard Harte	Oct 9 1894	Typewriting machine attachment for writing and translating messages in cipher
527,518 Alfred Weaver	Oct 16 1894	Secret telegraphy
530,082 Louis D. Bliss	Dec 4 1894	Telegraph key
533,804 Nicholas J. Halpine	Feb 5 1895	Pyrotechnic signaling
537,738 Lionel Wells	Apr 16 1895	Signaling apparatus
539,421 Roy O. Crowley	May 21 1895	Signaling apparatus
540,772 Charles Wilioughby	Jun 11 1895	Photo-telegraph
546,035 Georg Strömdal	Sep 10 1895	Cryptograph
563,148 Samuel V. Essick	Jun 30 1896	Telegraph alphabet
583,026 Charles G. Burke	May 25 1897	System of telegraphy
583,359 Frederic L. Dietz	May 25 1897	Negotiable paper and means for preventing counterfeiting thereof
584,462 Alvah L. Creelman	Jun 15 1897	Electric circuit protector
597,587 James Nicolson	Jan 18 1898	Telegraphic signal
599,742 Leopold Sellner	Mar 1 1898	Apparatus for visible signaling
600,917 Joseph J. Kulage	Mar 22 1898	Blank for negotiable instruments
621,767 Frederick Hachmann	Mar 21 1899	Check-protector
625,188 Robert McKeighan	May 16 1899	Cipher writer
630,847 Eugen A. Bofinger	Aug 15 1899	Typewriter ciphograph
630,848 Eugen A. Bofinger	Aug 15 1899	Typewriter ciphograph
637,049 William C. Van Horn	Nov 14 1899	Cryptographic chart
641,004 John W. Follansbee	Jan 9 1900	Instrument for secret writing and translating
641,481 Giovanni B. Valvasori	Jan 16 1900	Cipher apparatus
642,721 Willis J. Roussel	Feb 6 1900	Cipher code system
644,165 William A. Freret, Jr.	Feb 27 1900	Cryptographic typewriting machine
644,166 William A. Freret, Jr. et al.	Feb 27 1900	Cryptographic typewriting machine
650,716 Carroll E. Gates	May 29 1900	Method of and means for secret correspondence
650,830 Bradley A. Fiske	Jun 5 1900	Day signaling apparatus
654,834 George H. Landgraf	Jul 31 1900	Secret telegraph sounder
657,586 Elmer F. Cassel	Sep 11 1900	Cipher-code system
657,587 Elmer F. Cassel	Sep 11 1900	Cipher-code

UNITED STATES CRYPTOGRAPHIC PATENTS

(No Model.)

T. GRUAZ.
COMBINATION CIPHER.

No. 283,383.

Patented Aug. 28, 1883.



Fig. 1.

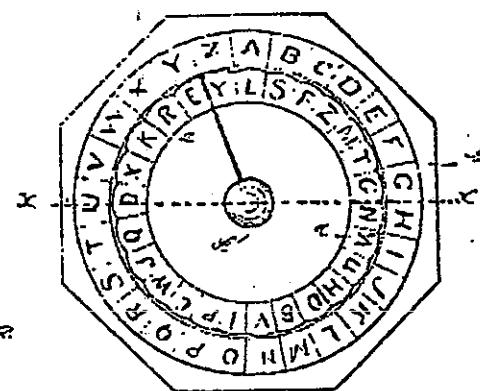


Fig. 3.

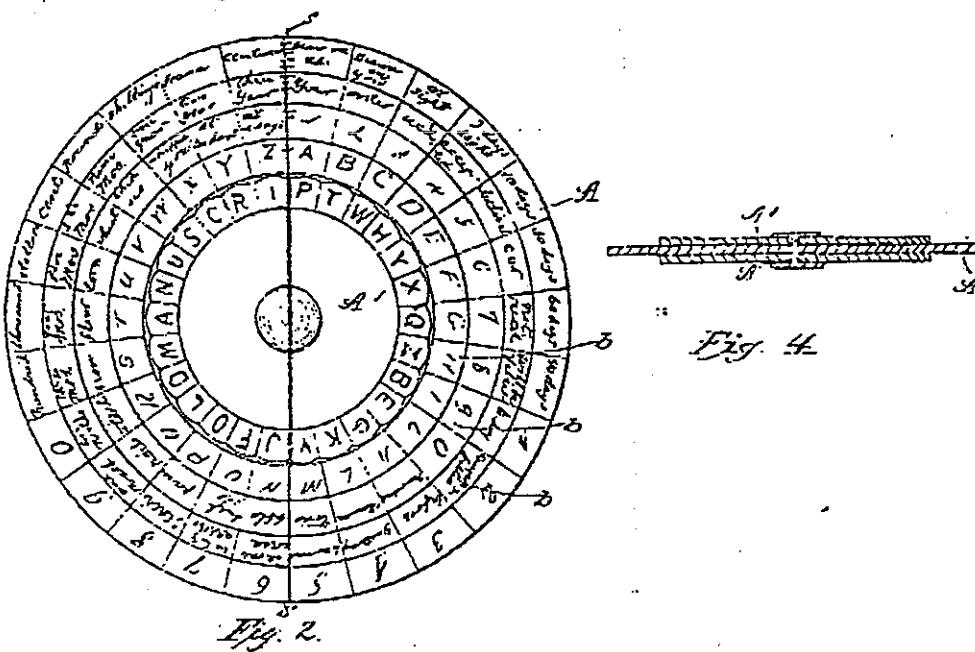


Fig. 4.

Witnesses:
Wm. Russell
J. Bernhard.

Inventor:
Timothy Gruaz
per -
Edwards Bros.
Atty's -

UNITED STATES CRYPTOGRAPHIC PATENTS

662,333 Joseph P. Angell	Nov 20 1900	Type-writer
665,402 John Burry	Jan 8 1901	Cryptographic type
666,176 George C. Blickensderfer	Jan 15 1901	Type-writing machine
666,520 Charles P. Hall	Jan 22 1901	Cipher code system
670,697 Frederick Bedell	Mar 26 1901	System of telegraphy
676,936 Charles G. Burks	Jun 25 1901	Telegraphic code
678,363 Adolphus W. Greely	Jul 16 1901	Telegraph and cable code
695,999 Richard Beger	Mar 25 1902	Type-writing machine
703,391 James E. Dempsey	Jul 1 1902	Telegraphic code
706,740 Reginald A. Fessenden	Aug 12 1902	Wireless signaling
715,686 Thomas D. Penniman.	Dec 9 1902	Electric telegraph
717,978 Cornelius D. Ehret	Jan 6 1903	Wireless selective signaling system
723,288 Harry S. Lewis	Mar 24 1903	Cipher key for cryptographic codes
723,566 Lewis H. Weston	Mar 24 1903	Cryptograph
724,786 Stephen T. Beveridge	Apr 7 1903	Cipher code system
725,634 John S. Stone	Apr 14 1903	Art of wireless or space telegraphy
725,635 John S. Stone	Apr 14 1903	Space telegraphy
725,636 John S. Stone	Apr 14 1903	Space telegraphy
727,213 Frederick Sedgwick	May 5 1903	Cipher type-writer
727,915 George W. Dudley	May 12 1903	Apparatus for cipher writing
737,203 Charles L. Buckingham	Aug 25 1903	Automatic printing telegraph
738,725 Simon Lake	Sep 8 1903	System of submarine communication
739,398 Alfred L. Day	Sep 22 1903	Cryptographic perforator
739,399 Alfred L. Day	Sep 22 1903	Cryptographic perforator
744,041 Charles G. Burke	Nov 17 1903	Telegraphic code
751,294 Arthur T. Johnson	Feb 2 1904	Apparatus for electrically transmitting and receiving messages
	Apr 5 1904	Code-index
756,209 Charles G. Burke	Apr 5 1904	Code-index
756,468 Charles G. Burke	Jul 19 1904	Machine for perforating telegraph tapes
765,456 Charles L. Buckingham et al.		
770,229 Lee de Forest	Sep 13 1904	Wireless signaling apparatus
791,209 Edmund Peycke	May 30 1905	Marginal and sub index for telegraphic cipher codes
793,037 Isidor Kitsee	Jun 20 1905	Electric telegraphy
797,016 Francisco Pimental	Aug 15 1905	Code system
801,964 Joseph S. Beeman	Oct 17 1905	Machine for coding and decoding messages
802,740 Patrick B. Delany	Oct 24 1905	Electromagnetic perforator for perforating electric-telegraph transmission-tapes
823,176 Isidor Kitsee	Jun 12 1906	Electric telegraphy
826,472 Charles L. Buckingham et al.	Jul 17 1906	Telegraphy
831,061 Daniel C. Gurnee	Sep 18 1906	Cipher code or system
831,968 Charles J. Mitchell	Sep 25 1906	Self-testing safety-code
832,156 Ernest E. Peterson	Oct 2 1906	Cipher-code
832,559 Ernest E. Peterson	Oct 2 1906	Cipher-code
833,904 Daniel H. Wilcox	Oct 23 1906	Telegraphic code
841,616 Harold H. Brown	Jan 15 1907	Signal reading device
841,885 Charles W. McDonald	Jan 22 1907	Telegraph code
841,952 Alexander M. Fisher	Jan 22 1907	Telegraphic code
842,106 Charles W. McDonald	Jan 22 1907	Code or cipher system
842,763 Hubert Burg	Jan 29 1907	Cryptographic machine
845,515 Hubert Burg	Feb 26 1907	Cryptograph

UNITED STATES CRYPTOGRAPHIC PATENTS

847,157 Harold G. Brown et al.	Mar 12 1907	Signaling apparatus
847,767 Martin C. Harlan	Mar 19 1907	Secret code apparatus
850,091 Frederick W. Lietzow	Apr 9 1907	Telegraph and cable cipher code
875,070 Carl Haas et al.	Dec 31 1907	Apparatus for correspondence in cipher
877,555 Patrick B. Delany	Jan 28 1908	Telegraphy
877,797 Frederick Pain	Jan 28 1908	Cable or telegraph code
879,667 Henry C. Newton et al.	Feb 18 1908	Cipher system
880,905 Bedford McNeill	Mar 3 1908	Tabulated gage for telegraphic or secret codes
889,094 Michael Berardini	May 26 1908	Code message
889,095 Michael Berardini	May 26 1908	Code message
894,378 Lee de Forest	Jul 28 1908	Wireless signaling apparatus
894,820 Patrick B. Delany	Aug 4 1908	Telegraphy
901,957 Matthew B. Dickie	Oct 27 1908	Telegraphic-code condenser
906,618 Patrick B. Delany	Dec 15 1908	Perforator for preparing telegraphic transmitting tapes
916,606 Willis J. Roussel	Mar 30 1909	Cipher-code system
916,899 Mortimer L. Sweeney	Mar 30 1909	Cable or telegraph code
927,641 John H. Cuntz	Jul 13 1909	Wireless telegraphy
933,679 Mortimer L. Sweeney	Sep 7 1909	Telegraph or cable code
935,536 Henry C. Newton et al.	Sep 28 1909	Apparatus for use in connection with check cipher systems
962,709 Isidor Kitsee	Jun 28 1910	Telegraphy
963,062 Walter P. Phillips	Jul 5 1910	Secret telegraph system
970,716 Clarence H. Keehn.	Sep 20 1910	Cable code system
971,170 Charles G. Burke	Sep 27 1910	Telegraphy
981,845 Patrick B. Delany	Jan 17 1911	Telegraphy
983,482 William Coyne et al.	Feb 7 1911	Cipher-code
984,832 Frank R. McBerty	Feb 21 1911	Cryptograph machine
986,400 Charles W. McDonald	Mar 7 1911	Telegraphic code concentrator
988,879 Isidor Kitsee	Apr 4 1911	Telegraphy
990,021 Mary E. Sweeney	Apr 18 1911	Cable or telegraph code
991,837 Simon Eisenstein	May 9 1911	Wireless signaling system
997,890 Samuel M. Wilson	Jul 11 1911	Telegraph-code system
998,833 Harry W. Bodwell	Jul 25 1911	Code-changing system
1,003,361 Serge Kanschine	Sep 12 1911	Type-writing machine
1,021,189 Irving Hill	Mar 26 1912	Alphabetical symbols
1,038,556 Erwin W. Fuller	Sep 17 1912	Machine for enciphering and deciphering messages
1,048,708 Charles H. Koerner	Dec 31 1912	Protected blank
1,057,223 Sloan Danenhower	Mar 25 1913	Visual signal for submarines
1,070,342 Fred Hoffman	Aug 12 1913	Combination code card
1,084,010 Edward H. Hebern	Jan 13 1914	Machine for forming code messages
1,085,636 Frederick Sedgwick	Feb 3 1914	Cipher type-writer
1,086,586 Charles G. Burke	Feb 10 1914	Code-forming device
1,086,823 Edward H. Hebern et al.	Feb 10 1914	Cryptographic attachment for type-writing machines
1,091,768 Frederick G. Sargent	Mar 31 1914	Method of and apparatus for selective wireless telegraphy
1,093,372 James C. Allum et al.	Apr 14 1914	Reversible typewriter key
1,096,168 Edward H. Hebern	May 12 1914	Means for interpreting code messages
1,102,442 Frederick G. Sargent	Jul 7 1914	Apparatus for selective wireless telegraphing

UNITED STATES CRYPTOGRAPHIC PATENTS

1,106,788 Sloan Danenhower	Aug 11 1914	Signaling apparatus
1,108,147 Patrick B. Delany	Aug 25 1914	Telegraphy
1,108,148 Patrick B. Delany	Aug 25 1914	Telegraphy
1,111,695 Abraham N. Hovland	Sep 22 1914	Type printing telegraph apparatus for line and radio telephony
1,120,784 Karl Ammon	Dec 15 1914	Cipher type-writer
1,123,119 Lee de Forest	Dec 29 1914	Secrecy system for wireless communication
1,123,738 Edward H. Hebern et al.	Jan 5 1915	Cryptographic attachment for typewriting machines
1,126,463 Edward H. Hebern	Jan 26 1915	Check-identifying machine
1,135,452 Edward H. Hebern	Apr 13 1915	Machine for interpreting code messages
1,136,875 Edward H. Hebern	Apr 20 1915	Cryptographic code cards
1,136,876 Edward H. Hebern	Apr 20 1915	Cipher-code device
1,138,832 Ottomar F. Bamberg et al.	May 11 1915	Writing machine
1,138,851 Benjamin M. Des Jardins	May 11 1915	Cryptograph
1,141,055 Edward H. Hebern	May 25 1915	Cipher-writing machine
1,149,428 Patrick B. Delany	Aug 10 1915	Telegraphy
1,149,803 Karl Ammon	Aug 10 1915	Cryptographic type-writing machine
1,152,808 Ramón Guzmán M.	'Sep 7 1915	Cryptographic apparatus
1,170,969 Reginald A. Fessenden	Feb 8 1916	Means of transmitting intelligence
1,182,179 Charles L. Krum et al.	May 9 1916	Perforator for forming telegraphic tape
1,189,277 Richard C. Martens	Jul 4 1916	Apparatus for coding messages.
1,195,701 James C. H. Macbeth et al.	Aug 22 1916	Codes, ciphers, and the like
1,196,338 Harry A. Corbett et al.	Aug 29 1916	Cryptographic machine
1,201,486 Sydney T. Maryc	Oct 17 1916	Code or cipher transcribing and translating mechanism
1,204,929 Henry M. Ball, Sr.	Nov 14 1916	Printing-machine for code communication
1,210,656 Samuel M. Kintner	Jan 2 1917	Apparatus for coding and decoding
1,214,022 Philip E. Edelman	Jan 30 1917	Apparatus for wireless telephony and the like
1,219,634 George C. Fisher	Mar 20 1917	Draft, check, money order, and other negotiable instrument
1,222,010 James E. Mack	Apr 10 1917	Printed instrument
1,233,035 Arvid G. Damm	Jul 10 1917	Apparatus for producing series of signs
1,233,715 Frederick Sedgwick	Jul 17 1917	Cipher typewriter
1,244,477 Patrick B. Delany	Oct 30 1917	Telegraphy
1,267,640 Frank W. Engelston	May 28 1918	Writing paper, card, tablet, or the like
1,271,000 John W. Wulf	Jul 2 1918	Code device
1,276,616 Paul Bienvaux	Aug 20 1918	Telegraphic-code apparatus
1,285,567 Ramón Guzmán M.	Nov 19 1918	Cryptographic method and apparatus
1,309,459 John R. Carson	Jul 8 1919	Wireless signaling system
1,310,719 Gilbert S. Vernam	Jul 22 1919	Secret signaling system
1,311,457 Luigi Nicoletti	Jul 29 1919	Cipher apparatus
1,312,572 Ralzemond D. Parker	Aug 12 1919	Secret-signaling system
1,312,574 Ralph E. Pierce	Aug 12 1919	Secret-signaling system
1,315,406 James Powers	Sep 9 1919	Apparatus and method for formulating and translating codes
1,318,366 Cosmo Farquhar	Oct 14 1919	Table for coding, decoding, and checking communications
1,320,908 Ralzemond D. Parker	Nov 4 1919	Ciphering and deciphering mechanism
1,322,010 Olof D. Guthe	Nov 18 1919	Telegraph system
1,325,574 Harold W. Nichols	Dec 23 1919	Secret signaling system
1,326,522 Joseph Marshall	Dec 30 1919	Signaling apparatus

UNITED STATES CRYPTOGRAPHIC PATENTS

1,332,861 George H. Williams	Mar 2 1920	Code record
1,350,789 Patrick B. Delany et al.	Aug 24 1920	Apparatus for treating telegraph tape
1,352,116 George C. Cummings	Sep 7 1920	Telegraphy
1,356,277 John C. Grant	Oct 19 1920	Typewriting machine for coding and decoding messages
1,356,546 Lyman F. Morehouse	Oct 26 1920	Ciphering system
1,356,592 John H. Bell	Oct 26 1920	Telegraph system
1,356,701 Augustus J. Eaves	Oct 26 1920	Secret telegraphic system
1,364,078 Albert C. Crehore	Jan 4 1921	Telegraphic alphabet or code
1,364,725 Jo�o N. Correia	Jan 4 1921	Telegraph system
1,367,311 A. R. Fergusson	Feb 1 1921	Means for mechanical indexing
1,367,717 Paul M. Rainey	Feb 8 1921	Printing telegraph system
1,369,805 Baxter P. Hamilton	Mar 1 1921	Secret communication system
1,370,870 Petro Zurawiecki	Mar 8 1921	Code reading instrument
1,372,797 George Bonnell	Mar 29 1921	Code-book
1,379,551 Henry C. Gauss	May 24 1921	Cryptography
1,379,905 Thomas M. Down	May 31 1921	Method of analyzing, transmitting, and reconstructing pictures or the like
1,387,261 Louis Harmuth	Aug 9 1921	Illustrated code
1,388,049 Joseph Koffend, Sr.	Aug 16 1921	Safety-check
1,389,559 James P. Griffiths	Aug 30 1921	Coding and decoding device
1,394,439 Donald Murray	Oct 18 1921	Code transposing apparatus for telegraph systems
1,395,378 Richard H. Wilson et al.	Nov 1 1921	Secret signaling
1,406,775 Charles M. Swingle	Feb 14 1922	Mesograph
1,414,496 Peter G. Beyer	May 2 1922	Cryptographic typewriter
1,415,106 Lyman F. Morehouse	May 9 1922	Ciphering device
1,416,765 Gilbert S. Vernam	May 23 1922	Ciphering device
1,420,257 John H. Hammond, Jr.	Jun 20 1922	System and apparatus for automatic wave selection
1,420,931 Edward E. Kleinschmidt	Jun 27 1922	Keyboard tape perforator
1,426,669 Ralph E. Pierce	Aug 22 1922	Ciphering device
1,426,944 Ernst F. Alexanderson	Aug 22 1922	Radiosignaling system
1,433,144 Bernhard Mora	Oct 24 1922	Code sign translator
1,437,325 Harry G. Telling	Nov 28 1922	Mechanical coding and decoding or ciphering apparatus
1,440,510 Ralph W. Trueblood et al.	Jan 2 1923	Device for coding and decoding telephotographs
1,440,585 Hamlet Corrigan	Jan 2 1923	Check protecting system and keyboard for same
1,441,109 Allen Newell	Jan 2 1923	Coding and decoding device
1,441,239 Charles C. Murray	Jan 9 1923	Cryptographic marking means
1,442,819 Ralzemon D. Parker	Jan 23 1923	Ciphering machine
1,445,605 Blas C. Silva	Feb 13 1923	Code
1,454,532 William E. Beatty	May 8 1923	Method of and means for secret signaling
1,455,157 Charles F. Wood	May 15 1923	Code table
1,460,438 Ralzemon D. Parker	Jul 3 1923	Secret communication system
1,461,783 Ralzemon D. Parker et al.	Jul 17 1923	Secret communication system
1,463,994 John H. Hammond, Jr.	Aug 7 1923	System for the transmission and reception of radiant energy
1,464,086 William E. Beatty	Aug 7 1923	Method of and means for secret signaling
1,464,096 Ralph V. Hartley	Aug 7 1923	Secret signaling
1,465,368 William J. Shackelton	Aug 21 1923	Secret signaling system
1,470,594 David E. Branson	Oct 16 1923	Secret signaling system

UNITED STATES CRYPTOGRAPHIC PATENTS

(No Model.)

G. STRÖMDAL.
CRYPTOGRAPH.

No. 546,035.

Patented Sept. 10, 1895.

Fig. 2.

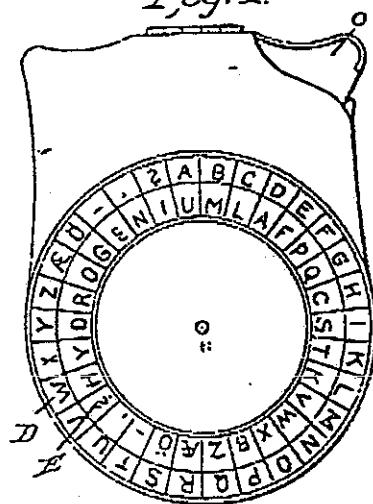


Fig. 3.

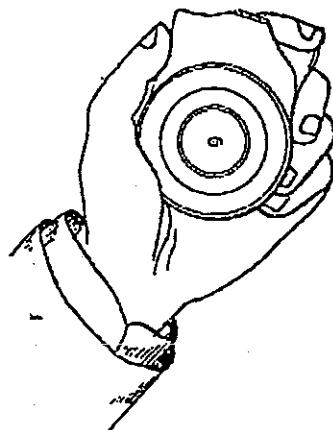


Fig. 4.

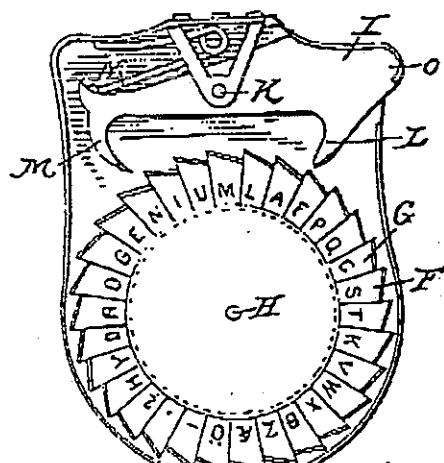
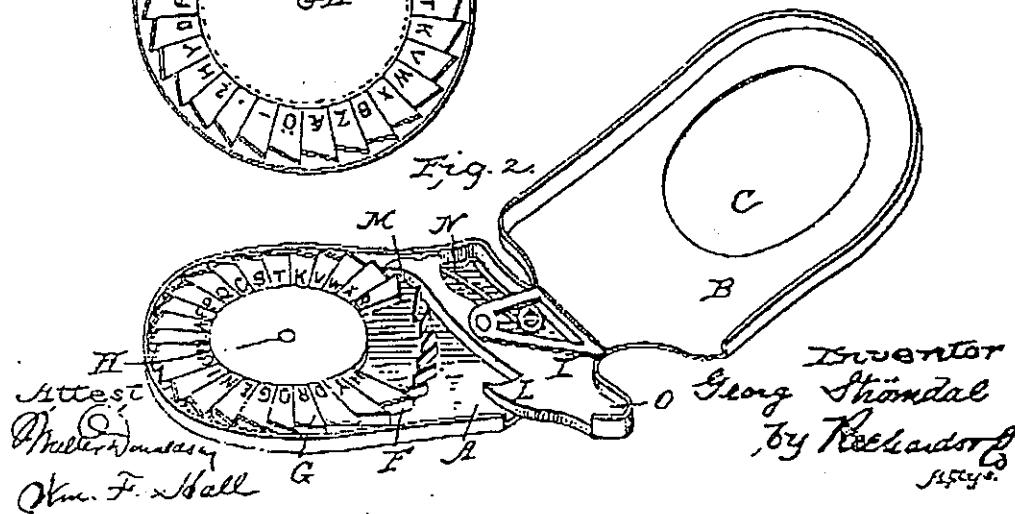


Fig. 2.



B



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO.
860,586	12-14-77	Ronald L. Rivest, et al.	

- Arthur A. Smith, Jr.
Mass. Institute of Technology
Room E19-722
Cambridge, Mass. 02139

EXAMINER	
H.A. Birmiel	
ART UNIT	PAPER NUMBER
222	10
DATE MAILED:	

EXAMINER INTERVIEW SUMMARY RECORD

All participants (applicant, attorney, agent) representing applicant:

(1) MR. LAPPIN (3) _____
 (2) _____ (4) _____

AUG 6 1979

Date of interview _____

GROUP 220

Type: Telephonic Personal (copy is given to applicant).

Exhibit shown or demonstration conducted: Yes No.

Agreement was reached with respect to some or all of the claims in question. was not reached.

Claims discussed: 1-33, 34-35

Identification of prior art discussed: _____

Description of the general nature of what was agreed to if an agreement was reached, or any other comments: _____

APPLICANTS' ATTORNEY AGREED TO AMEND THE CLAIMS TO REFLECT THAT THE MATHEMATICAL TRANSFORMATIONS WERE PERFORMED UPON "SIGNALS" TO BETTER DEFINE THE SAME IN LIGHT OF THE 35USC101 REJECTION WHICH IS WITHDRAWN. CLAIMS 34-35 ARE TO BE AMENDED TO REMOVE MULTIPLE DEPENDENCY.

(A fuller necessary description and any available copy of amendments that the examiner agreed would render the claims allowable, or where no copy of the amendments is available, a summary thereof, is attached.)

It is not necessary for applicant to supplement the information on this form or to submit a separate record of the interview.

Howard A. Birmiel
HOWARD A. BIRMIEL
EXAMINER

APPLICANTS, ATTORNEYS AND AGENTS ARE REMINDED OF THEIR RESPONSIBILITY TO SUPPLEMENT THIS RECORD WITH AN INDICATION OF THE SUBSTANCE OF THE INTERVIEW AS REQUIRED BY 37 CFR 1.133(b) AND SECTION 713.04 OF THE MANUAL OF PATENT EXAMINING PROCEDURE. (See reverse side for text of Section 713.04.)



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

80-00 - 1112 68-282

In the matter of the application of :
Ronald L. Rivest, Adi Shamir and :
Leonard M. Adleman :
Serial No: 860,586 ✓ :
Filed: December 14, 1977 :
For: CRYPTOGRAPHIC COMMUNICATIONS :
SYSTEM AND METHOD :

Examiner: H.A. Birmiel

Group Art Unit: 222

RECEIVED

MAY 23 1979

GROUP 220

Hon. Commissioner of Patents
Washington, D.C. 20231

Dear Sir:

This paper is responsive to the Office Action of December 15, 1978. Please amend the above-referenced application as follows:

IN THE CLAIMS:

Add the following claims:

Sub
C.2
multiple copies
List before 01-04-78
B-1
34. A system according to claims 1 or 2 or 3 or 4 or 5 or 6 or 7 or 8 or 9 or 10 or 11 or 12 or 13 or 14 or 15 or 16 or 17 or 28 or 29 or 30 wherein at least one of said transforming means comprises:

a first register means for receiving and storing a first digital signal representative of said word-to-be-transformed,

a second register means for receiving and storing a second digital signal representative of the exponent of the equivalence relation defining said transformation,

a third register means for receiving and storing a third digital signal representative of the modulus of the equivalency relation defining said transformation, and

-2-

05.22.79 12-18

5934 115/301

OK 768
3. 1980 K 557

an exponentiation by repeated squaring and multiplication network coupled to said first, second and third register means, said network including:

- A. an output register means for receiving and storing a first multiplier signal and for applying said first multiplier signal to a first multiplier input line,
- B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,
- C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying multiplier signal to a second multiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and
- D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals and for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary 1, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.

40 : 24 25 26 27
38. A method according to claims 18 or 19 or 20 or 21 or 22 or
28 24 30 31 32 33 34 35 36 37 38 39
23 or 24 or 25 or 26 or 27 or 31 or 32 or 33 wherein at least one
of said transforming means comprises the steps of:

receiving and storing a first digital signal in a first register, said first digital signal being representative of said word-to-be-transformed,

receiving and storing a second digital signal in a second register, said second digital signal being representative of the exponent of the equivalence relation defining said transformation,

receiving and storing a third digital signal in a third register, said third digital signal being representative of the modulus of the equivalency relation defining said transformation, and

exponentiating said first digital signal by repeated squaring and multiplication using said second and third digital signals, said exponentiating step including the substeps of:

- A. receiving and storing a first multiplier signal in an output register, and applying said first multiplier signal to a first multiplier input line,
- B. successively selecting each of the bits of said second digital signal as a multiplier selector, and
- C. for each of said multiplier selectors, selecting as a second multiplier signal either the contents of said output register or the contents of said first register, and for applying said second multiplier signal to a second multiplier output line, said selection being dependent on the binary value of the successive bits of said second digital signal,
- D. for each of said multiplier selectors, generating

said first multiplier signal in a modulo multiplier in response to the first and second multiplier signals on said first and second multiplier input lines, and for transferring said generated first multiplier signal to said output register, said first multiplier signal initially being representative of binary 1 and thereafter being representative of the modulo product of said first and second multipliers, where the modulus of said modulo product corresponds to said third digital signal.

REMARKS:

The applicants' attorney gratefully acknowledges the Examiner's efforts extended at the interview of March 2, 1979.

Initially, it is noted that new claims 34 and 35 have been added. These claims are directed to cover applicants' invention in the form shown in Fig. 3. As agreed to by the Examiner at the interview, Fig. 3 clearly has sufficient hardware to support allowable claims. Accordingly, it is submitted that claims 34 and 35 are at least allowable combined with the claims from which they depend.

In the Office Action, all of claims 1-33 were rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. Issue is taken with that position.

In the rejection, the Examiner states that "the present invention as claimed lies in a particular algorithm which is employed to implement the public key cryptography scheme of Diffie and Hellman (reference R). However, there are no mathematical algorithms in the applicants' claims.

The expressions in the applicants' claims which include

the symbol " \equiv " denote the well-known equivalence relation: congruence modulo m , for integers. The symbol " \equiv " merely is a shorthand notation (invented by Gauss in 1801) for expressing this equivalence relation to relate sets of numbers shown on either side of that symbol, in effect establishing a set of conditions between the related integers, or signals representative thereof. In Van Norstrand's Scientific Encyclopedia (Van Norstrand Reinhold Company, 1976, page 64), this equivalence relation is defined as follows:

Two elements a, b of a ring are congruent modulo m , written $a \equiv b \pmod{m}$, if there exist elements p, q, r in the ring such that $a = mp+r$, $b = mq+r$

Also see Stewart, B.M., Theory of Numbers, MacMillan Company, New York, 1952, pages 111, 112 (copy enclosed). Thus, the symbol " \equiv " is a symbol for "congruence", not arithmetic or mathematical "equality", and the fact that the equivalence relation of the form

$$A \equiv B^C \pmod{n}$$

is in the claims does not introduce a mathematical formula or algorithm to the claims but rather describes a relationship between two signals, e.g. the message and ciphertext. More particularly, in the applicants' claims, the message M and the ciphertext C are related by the transformation performed by the encoding means and the ciphertext C is related to the receive message word M' by the transformation performed by the decoding means. The claims include a description of these relationships, but do not specify any algorithms for effecting the transformations.

It should be noted that there may be many algorithms

which may be used to obtain the various terms for the relation. For example, the "exponentiation by repeated squaring and multiplication" approach shown by applicants' in the preferred embodiment is but one way of finding terms satisfying the relation. However, applicants do not claim any particular algorithms. In fact, any algorithms which may be used in practicing applicants' invention may readily be used in other applications without being covered by the applicants' claims.

Thus, the applicants' claimed invention does not "lie in an algorithm" which is employed to implement the Diffie and Hellman scheme, as characterized by the Examiner, but rather resides in a step of or means for transforming an input signal to an output signal in a communications system so that the output signal is related to the input signal by the specified equivalency relation, regardless of the particular technique or algorithm employed in performing that transformation.

Moreover, it appears that the §101 rejection would not have even come into play in this case if the expressions of the equivalency relation were not present. This may be seen if it is assumed for the moment that the encoding and decoding (i.e. transforming) means of claim 1 were simple transformation means, for example, digital complimenting or inverter circuits. Then, the claim could have the form:

A cryptographic communications system comprising:

- A. a communications channel
- B. an encoding means coupled to said channel including means for digitally inverting a transmit message word M to form a ciphertext word C and for transmitting C on said channel
- C. a decoding means coupled to said channel and adapted for receiving C from said

channel and for inverting C to form a receive message word M'.

This hypothetically claimed system has three basic elements: a communication channel and two inverters coupled thereto. The inverters perform a "mathematical transformation" on the signal applied to them. There is no algorithm specified for performing the inversion, but only a requirement that the ciphertext be related to the message by the complementing relation.

Assuming that digital complementing was a suitable transformation for the invention, and that the claimed structure satisfied 102 and 103, then there would be no question that the claims would be allowable. Section 101 would quite properly not come into play since there are merely three interconnected hardware elements. In the present case, the encoding and decoding means are merely somewhat more complex building blocks than inverter circuits, where each block performs a transformation on input signals applied to the block. As in the hypothetical claim, there is no particular formula or algorithm specified for the transformation in the applicants' claims--only that the resultant signal be related to the input signal by the stated equivalency relation.

The applicants merely use such a building block. While at the present time there may not be any single chip implementations of that building block available, the block may be readily built by those skilled in the art, for example by merely implementing the circuit shown in Fig. 3. The applicants by their claims certainly do not preempt the transformation performed by the building block. For these reasons, the Examiner's position that the claimed invention "lies in a particular algorithm" is incorrect. Accordingly, the rejection should be

reconsidered and withdrawn.

It is also noted that the rejection was applied against claims 1-17 and 28-30 which are system claims, as well as claims 18-27 and 31-33 which are method claims.

Regarding the method claims 18-27 and 31-33, the Examiner stated that the "invention as claimed lies in a particular algorithm . . .", citing Parker v. Flook, 198 U.S.P.Q. 193 and Gottschalk v. Benson, 175 U.S.P.Q. 673. The Examiner appears to use the term "algorithm" synonymously with the term "mathematical formula" found, for example, in the Benson case. The present invention, as claimed, does not fall within the proscribed subject matter of the Benson case, because it does not seek to patent a mathematical formula, and hence does not seek to patent an "algorithm" within the definition of mathematical formula set forth by Benson and Flook. As noted above, the claims 18-27 and 31-33 do not claim mathematical formulae but merely include expressions of an equivalence relation to pose conditions (expressed in Gauss' shorthand notation) on the claimed transformations.

The Court in Flook noted that "the only novel feature of the method is a mathematical formula", 198 U.S.P.Q. at 195. The Court goes on to state in footnote 1 on page 195 that "we use the word "algorithm" in this case as we did in Gottschalk v. Benson, . . ., to mean "a procedure for solving a given type of mathematical problem...". The subject matter claimed in the present case is neither a procedure for solving a mathematical problem, nor a hitherto unknown mathematical formula or a sequence of such mathematical formulae, but is instead the application of one or more process steps to establish cryptographic communications and to provide authentication of digital messages.

While some of these steps may be, and in fact are, expressed in part with an equivalence relation (i.e. using Gauss' shorthand notation), that fact does not implicate that those steps are claims to a mathematical formula or algorithm. In the present case, the applicants' claimed steps do not claim a mathematical formula or algorithm. This may be better seen if, for example, lines 13 and 14 of claim 18 were changed from "whereby $C \equiv M^e \pmod{n}$ " to an equivalent form which reads "by selecting C so that the difference between C and the e th power of M is an integer multiple of n." Clearly, there is no "algorithm" in this form of the claim. It does not matter how C is selected. For example, C may be selected by "trial-and-error", or alternatively by "exponentiation-by-repeated-squaring" (as in the applicants' preferred embodiment) or some other method. The exponentiation-by-repeated-squaring approach is of course considerably more efficient in terms of hardware implementation. But it is important to note that the claims are independent of any particular method (or algorithm) for finding the terms to satisfy the relation. All that matters is that these terms be found -- by any method or algorithm. This same reasoning is applicable to all of claims 1-33. Thus, the claimed invention is not a proscribed "algorithm" within 35 U.S.C. 101.

The CCPA cases which have evolved in the face of Benson and Flook (and which have not been reversed), cases such as In re Chatfield, 191 USPQ 730 (CCPA 1976), In re Freeman, 197 USPQ 464 (CCPA 1978), and In re Johnson, et al., 200 USPQ 199 (CCPA 1978), clearly support the proposition that the invention claimed herein is patentable under 35 U.S.C. 101. The Johnson decision (which was handed down after the Office Action herein) is particularly informative since it follows (in time and substance) the Flook

decision. In Johnson, the CCPA states:

"[I]t is clear after Flook that the board's conclusion that patent protection is proscribed for all inventions algorithmic in character is overbroad and erroneous."
(200 USPQ at 205)

The CCPA in Johnson further went on to solidify the definition of an algorithm, citing Chatfield, wherein they stated:

"The Supreme Court carefully supplied a definition of the particular algorithm before it, i.e., [a] procedure for solving a given type of mathematical problem.

"The broader definition of algorithm is a step-by-step procedure for solving a problem or accomplishing some end.... It is axiomatic that inventive minds seek and develop solutions to problems and step-by-step solutions often attain the status of patentable invention. It would be unnecessarily detrimental to our patent system to deny inventors patent protection on the sole ground that their contribution could be broadly termed an 'algorithm'."
(200 USPQ at 206-207)

The CCPA then went on to review the two step analytical approach taken in Freeman to determine whether or not the claims before it were patentable. The Court of Customs and Patent Appeals in Freeman dealt with method claims similar in form to the method claims rejected in the present case. The CCPA's analysis in that decision is directly applicable here. In Freeman, the Court set forth a two-step analysis for determination of whether a claim is directed to non-statutory subject matter as a whole, in light of Benson:

"First, it must be determined whether the claim directly or

indirectly recites an 'algorithm' in the Benson sense of that term,....

"Second, the claim must be further analyzed to ascertain whether in its entirety it wholly preempts that algorithm." (197 USPQ at 471)

In Freeman, the Court noted that every process may be characterized as a "step-by-step procedure...for accomplishing some end" and that therefore, it would be "absurd" to interpret the Supreme Court's view as encompassing all such processes. Even if that "absurd" interpretation were taken, in the present case, as discussed above, the rejected claims are not "algorithmic", in spite of the fact that the claims include an equivalence relation. That equivalence relation only expresses conditions on a transformation. The conditions expressed by that equivalence relation may not be characterized as "a step-by-step procedure...for accomplishing some end". Thus, the present rejection should be reconsidered and withdrawn for the same reasons cited in Freeman.

Even assuming that according to the first step of Freeman analysis, the process steps herein "directly or indirectly recite process steps which are themselves calculations, formulae, or equations" (which in applicants' opinion they do not), it is clear that the applicants' claims in no way wholly preempt any such calculations, formulae or equations. This may be seen, for example, by the fact that a congruency equivalence relation is found in the cipher system disclosed by the Stewart reference (copy enclosed with the applicants' prior art statement), but Stewart's approach is clearly not within the scope of the applicants' claims. Thus, the second step of the Freeman analysis leads to the inevitable conclusion that the claims herein clearly fall squarely within the Johnson analysis

and the present claims should be allowed.

Furthermore, following the remainder of Johnson reasoning, the CCPA elaborates upon its two part Freeman analysis to determine whether the claims recite mathematical algorithms which are non-statutory. Under the continuing second step analysis of the CCPA's reasoning, one

"must determine whether each claim as a whole, including all of its steps, merely recites a mathematical formula or a method of calculation. This analysis requires careful interpretation of each claim in the light of its supporting disclosure to determine whether or not it merely defines a method of solving a mathematical problem. If it does not, then it defines statutory subject matter, namely, a 'process'".
(200 USPQ 208, 209)

The invention in claims 18-27 and 31-33 is not directed to the solution of a mathematical problem, but rather solves the problem of privately transmitting a message over a communications channel and the problem of authentication (i.e. by providing digital signatures) of messages. The claims include the step of transforming a first signal to a second signal so that the second signal is related to the first by a stated equivalence relation. The method for doing so does not claim mathematical formulae and does not seek patents on a mathematical formula. Accordingly, the invention claimed herein clearly falls under the CCPA and Supreme Court reasonings.

For these reasons, the rejection of claims 18-27 and 31-33 under 35 U.S.C. 101 should be reconsidered and withdrawn.

With particular regard to system claims 1-17, and 28-30, it is noted that the Benson and Flook cases cited by the Examiner addressed method claims only. The Supreme Court in

Benson stated "The question is whether the method described and claimed is a 'process' within the meaning of the Patent Act." 175 USPQ at 674 (emphasis added). Similarly, in Flook, the Supreme Court addressed the question of whether a novel formula "makes an otherwise conventional method eligible for patent protection" 198 USPQ at 196. Thus, in both of the cited cases, the Supreme Court addressed "processes" under 35 U.S.C. 101.

In contrast, the claims 1-17 and 28-30 are all directed to apparatus including means to perform specified functions. Moreover, the claims are clearly supported in the specification by a hardware implementation of the claimed subject matter. Accordingly, the rejection of system claims 1-17 and 28-30 is inappropriate and should be reconsidered and withdrawn.

Moreover, even if the Examiner treats these system claims in the same manner as the method claims 18-27 and 31-33, the rejection should be withdrawn for the reasons discussed above in particular reference to the method claims.

For these reasons, the rejection of claims 1-33 under 35 U.S.C. 101 is inappropriate and should be withdrawn. It is submitted that these claims, as well as new claims 34 and 35 are in condition for allowance and passage to issue is requested.

Respectfully submitted,

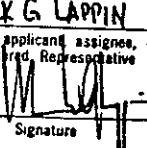
KENWAY & JENNEY

By

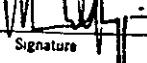

Mark G. Lappin
Reg. No. 26,618

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D. C. 20231.

on MAY 15 1979
(Date of Deposit)


MARK G. LAPPIN

Name of applicant, assignee, or
Registered Representative


MAY 15 1979

Date of Signature

60 State Street
Boston, MA 02109
Tel: (617)227-6300
May 15, 1979



RECEIVED

MAY 23 1979

GROUP 220

May 15, 1979

In re application of Ronald L. Rivest, Adi Shamir and
Leonard M. Adleman

Serial No. 860,586

Filed December 14, 1977

For CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD

THE COMMISSIONER OF PATENTS
Washington, D.C. 20231

Sir:

Transmitted herewith is an amendment in the above-identified application.

No additional fee is enclosed because this application was filed prior to October 25, 1965 (effective date of Public Law 89-83.)
 No additional fee is required.

The fee has been calculated as shown below.

CLAIMS AS AMENDED						
	(2) CLAIMS REMAINING AFTER AMENDMENT	(3)	(4) HIGHEST NO. PREVIOUSLY PAID FOR	(5) PRESENT EXTRA	(6) RATE	(7) ADDITIONAL FEE
TOTAL CLAIMS	* 73	MINUS	** 33	= 40	x \$2	x \$80.00
INDEP. CLAIMS	* 10	MINUS	10	= 0	x \$10	x 0
TOTAL ADDITIONAL FEE FOR THIS AMENDMENT					\$80.00	

* If the entry in Column 2 is less than the entry in Column 4, write "0" in Column 5.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 10, write "10" in this space.

A check in the amount of \$ 80.00 is attached.

Charge \$ _____ to Deposit Account No. _____. A duplicate copy of this sheet is enclosed.

Please charge any additional fees or credit overpayment to Deposit Account No. 11-575. A duplicate copy of this sheet is enclosed.

Mark G. Lappin
Reg. No. 26,618